MACURA.

Chambers RANKED IN FinTech 2025 Kancelaria Macura

Rozporządzenie DORA - jak zadbać o cyberbezpieczeństwo w rozwiązaniach płatniczych?

Praktyczny przewodnik

Monika Macura
Michał Barwicki

#cyberbezpieczeństwo
#NoweTechnologie

SPIS TREŚCI

STRONA

Przedmowa autorów

Chambers RANKED IN FinTech 2025 Kancelaria Macura

W obliczu ciągłego postępu technologicznego i coraz większej digitalizacji rynków finansowych, nowe regulacje wprowadzają znaczące wyzwania dla całego sektora finansowego. Rozporządzenie DORA (Digital Operational Resilience Act) stanowi integralną część tej ewolucji, odpowiadając na specyficzne potrzeby związane z odpornością operacyjną w sektorze finansowym.

Cyberbezpieczeństwo, niegdyś zagadnienie ograniczone do działów IT, obecnie staje się kluczowym elementem strategicznym dla każdej organizacji w sektorze finansowym. Rozporządzenie to nie tylko wymusza na instytucjach finansowych implementację zaawansowanych technologii w zakresie cyberbezpieczeństwa, ale również wymaga od nich zrozumienia prawnego kontekstu oraz jego wpływu na działalność biznesową.

Radca prawny
Monika Macura

Radca prawny
Michał Barwicki

Zapewnienie zgodności z DORA wymaga interdyscyplinarnego podejścia, łączącego aspekty prawne, biznesowe i technologiczne, co dla wielu instytucji finansowych i ich dostawców ICT stanowić będzie kluczowe wyzwanie.

Mamy głęboką nadzieję, że niniejsza publikacja ułatwi zrozumienie tego, czym jest Rozporządzenie DORA, jakie stawia wymagania oraz jakie mogą być skutki konieczności wdrożenia Rozporządzenia DORA dla całego sektora finansowego, ze szczególnym uwzględnieniem branży fintech i lendtech.

Zrozumienie tych aspektów jest niezbędne do utrzymania konkurencyjności i dynamicznego rozwoju, przy równoczesnym minimalizowaniu ryzyka prawno-regulacyjnego.

Wprowadzenie

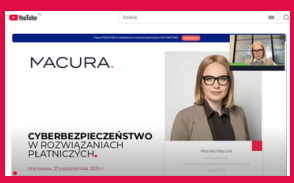
Cyberbezpieczeństwo w rozwiązaniach płatniczych wymaga zintegrowanego podejścia uwzględniającego jednocześnie regulacje prawne, zarządzanie ryzykiem, jak i najlepsze praktyki operacyjne.

Nowe regulacje, takie jak **wchodzące w życie 17 stycznia 2025 r. Rozporządzenie DORA,** podnoszą standardy bezpieczeństwa w sektorze finansowym, jednak ich skuteczność zależy od wdrożenia odpowiednich procedur oraz współpracy między instytucjami a dostawcami technologii.

Oddajemy do Państwa rąk praktyczny przewodnik, podsumowujący cykl webinarów oraz artykułów autorstwa **radców prawnych Moniki Macury** i **Michała Barwickiego**, poświęconych przygotowaniu do wdrożenia regulacji DORA w instytucjach finansowych, opublikowanych na blogu kancelarii Macura.

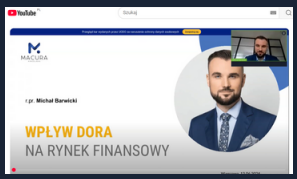
Webinaria na temat DORA

Zachęcamy do obejrzenia nagrań webinariów, poświęconych tematyce wdrożenia DORA, dostępnych na **kanale youtube Monika Macura Kancelaria Radcy Prawnego**:



Webinarium pt. **„Cyberbezpieczeństwo w rozwiązaniach płatniczych”** , które 21 października 2024 r. prowadziła radca prawny Monika Macura, na temat podstawowych zagrożeń, regulacji oraz dobrych praktyk w zakresie cyberbezpieczeństwa dla instytucji finansowych.

Webinarium pt. **„Wpływ rozporządzenia DORA na rynek finansowy”** , które 13 czerwca 2024 r. poprowadził **radca prawny Michał Barwicki**.



Digital Operational Resilience Act – najważniejsze definicje

W poniższym artykule, powstałym na podstawie webinarium, które 21 października 2024 r. prowadziła radca prawny Monika Macura, na temat podstawowych zagrożeń, regulacji oraz dobrych praktyk w zakresie cyberbezpieczeństwa dla instytucji finansowych, omawiamy podstawowe definicje zawarte w tzw. rozporządzeniu DORA (Digital Operational Resilience Act). Pełne nagranie webinarium „Cyberbezpieczeństwo w rozwiązaniach płatniczych" jest dostępne na kanale youtube kancelarii.

Operacyjna odporność cyfrowa

Oznacza zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej operacyjnej integralności i niezawodności przez zapewnianie, bezpośrednio albo pośrednio – korzystając z usług zewnętrznych dostawców usług ICT – pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość, w tym w trakcie zakłóceń.

Usługi ICT

To usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego, obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej.

Krytyczna lub istotna funkcja

Wskazuje funkcję, której zakłócenie w sposób istotny wpłynęłoby na:

- wyniki finansowe podmiotu finansowego;
- bezpieczeństwo lub ciągłość usług i działalności tego podmiotu;
- lub której zaprzestanie lub wadliwe bądź zakończone niepowodzeniem działanie w sposób istotny wpłynęłoby na dalsze wypełnianie przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych.

Incydenty związane z ICT

Incydent oznacza pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy.

- **Incydent operacyjny lub incydent w zakresie bezpieczeństwa związany z płatnościami**

  To zdarzenie lub seria powiązanych ze sobą zdarzeń, nieplanowanych przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a)–d) DORA, związanych z ICT lub nie, które mają negatywny wpływ na:
  - dostępność;
  - autentyczność;
  - integralność;
  - lub poufność

  danych związanych z płatnościami lub świadczonych usług związanych z płatnościami realizowanymi przez dany podmiot finansowy.

- **Poważny incydent związany z ICT,** który oznacza incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego.

- **Poważny incydent operacyjny lub poważny incydent w zakresie bezpieczeństwa związany z płatnościami**, czyli incydent operacyjny lub incydent w zakresie bezpieczeństwa związany z płatnościami o dużym negatywnym wpływie na świadczone usługi związane z płatnościami.

Ryzyko koncentracji w obszarze ICT

Jest równoznaczne z ekspozycją na poszczególnych lub wielu powiązanych ze sobą kluczowych zewnętrznych dostawców usług ICT, która prowadzi do takiego stopnia uzależnienia od takich dostawców, że niedostępność, awaria lub innego rodzaju braki po stronie tych ostatnich mogą potencjalnie zagrozić zdolności podmiotu finansowego do wypełniania krytycznych lub istotnych funkcji lub przyczynić się do poniesienia przez ten podmiot innego rodzaju negatywnych skutków, w tym dużych strat, lub zagrozić stabilności finansowej Unii jako całości.

Autor: Monika Macura, radca prawny

Cyberbezpieczeństwo w rozwiązaniach płatniczych

Cyberbezpieczeństwo w obszarze płatności jest kluczowym elementem ochrony danych i systemów wewnętrznych przed zagrożeniem cyberatakami. Wraz z rosnącą liczbą transakcji online wyzwaniem staje się zapewnienie bezpieczeństwa nie tylko systemów informatycznych, ale również danych osobowych i finansowych użytkowników.

W tym artykule omawiamy podstawowe zagrożenia, regulacje oraz dobre praktyki w zakresie cyberbezpieczeństwa dla instytucji finansowych.

Najistotniejsze zagrożenia w obszarze płatności

Systemy płatnicze są narażone na różnorodne zagrożenia, z których najczęstsze to:

- **złośliwe oprogramowanie (malware)**, obejmujące wirusy, trojany oraz oprogramowanie ransomware, które szyfruje dane i wymaga okupu za ich odszyfrowanie;
  ataki ransomware często wykorzystują techniki socjotechniczne, jak phishing lub vishing;
- **wyłudzanie informacji (phishing)**, w ramach którego cyberprzestępcy podszywają się pod pracowników instytucji finansowych, aby uzyskać dostęp do poufnych danych, takich jak hasła czy numery kart płatniczych;

- **inżynieria społeczna**, czyli manipulowanie ludźmi w celu uzyskania nieuprawnionego dostępu do chronionych informacji;
- **ataki typu DDoS (Distributed Denial of Service)**, które powodują przeciążenie serwerów, co skutkuje utratą dostępności usług;
- **spoofing**, obejmujący podszywanie się pod inny podmiot, np. dostawcę usług płatniczych, aby oszukać użytkownika i wyłudzić środki.

Zagrożenia te mogą prowadzić do poważnych strat finansowych, naruszenia prywatności oraz utraty reputacji przez instytucje finansowe.

Ransomware – specyfika i prewencja

Ransomware to jeden z najgroźniejszych rodzajów złośliwego oprogramowania, którego działanie polega na zaszyfrowaniu danych ofiary i żądaniu okupu za ich odblokowanie. Często takie ataki wykorzystują inżynierię społeczną. Ich przykładami są phishing i vishing, niepoprawnie zabezpieczone dostępy zdalne czy spoofing (w tym caller ID spoofing).

W maju 2024 r. Komisja Nadzoru Finansowego (KNF) wydała wytyczne dotyczące ochrony przed ransomware, których schemat obejmuje następujące etapy:

1. przygotowanie – zabezpieczenie systemów oraz szkolenie pracowników;
2. identyfikacja i szybkie wykrywanie prób ataków;
3. ograniczanie i minimalizowanie skutków ataku poprzez natychmiastowe działania;
4. komunikacja zewnętrzna i raportowanie;
5. odzyskiwanie i przywracanie danych z kopii zapasowych;
6. analiza incydentu i wdrożenie wniosków.

Nowe zasady odpowiedzialności dostawcy usług płatniczych za spoofing

Określa je Rozporządzenie w sprawie usług płatniczych w ramach rynku wewnętrznego PSR (Payment Service Regulation), określając spoofing jako podszywanie się przez oszustów pod pracownika dostawcy usług płatniczych.

Płatnik – ofiara spoofingu – uprawniony będzie do otrzymania od dostawcy usług płatniczych zwrotu pełnej kwoty nieuczciwej transakcji płatniczej, pod warunkiem zgłoszenia tego oszustwa organom ścigania, za wyjątkiem sytuacji, w których płatnik dopuścił się „nieuczciwego działania" lub „rażącego niedbalstwa".

Unijne regulacje w zakresie cyberbezpieczeństwa – DORA

W Unii Europejskiej kwestie związane z bezpieczeństwem cyfrowym w sektorze finansowym reguluje m.in. tzw. rozporządzenie DORA **(Digital Operational Resilience Act),** które **wchodzi w życie 17 stycznia 2025 r.**

DORA, która obok rozporządzeń MICA i DLT, stanowi część pakietu regulacji finansów cyfrowych, **ma na celu**:

- wzmocnienie odporności cyfrowej instytucji finansowych przez wprowadzenie jednolitych zasad bezpieczeństwa sieci i systemów;
- zobowiązanie podmiotów do raportowania poważnych incydentów związanych z technologią informacyjną;
- zapewnienie odpowiedniego zarządzania ryzykiem związanym z zewnętrznymi dostawcami usług ICT;
- nałożenie obowiązku przeprowadzania regularnych testów operacyjnej odporności cyfrowej, w tym testów penetracyjnych.

Rozporządzenie **obejmuje różnorodne podmioty, od banków i instytucji płatniczych po dostawców usług kryptowalutowych.**

Rozporządzenie DORA przewiduje też w pewnym zakresie odmienne, **uproszczone zasady, mające zastosowanie do niektórych podmiotów**:

- tzw. uproszczone ramy zarządzania ryzykiem związanym z ICT;
- uproszczone zasady przewidziane w przypadku niektórych wymogów i obowiązków dla mikroprzedsiębiorców (mikroprzedsiębiorcą będzie podmiot, który to zatrudnia mniej niż 10 osób i której roczny obrót lub bilans roczny nie przekracza 2 mln EUR).

Podstawowe wymogi DORA

Aby skutecznie chronić rozwiązania płatnicze przed cyberzagrożeniami, organizacje powinny stosować szereg **dobrych praktyk**, w tym:

- zarządzania ryzykiem ICT;
- zgłaszania poważnych incydentów związanych z ICT właściwym organom oraz dobrowolnego informowania ich o znaczących cyberzagrożeniach;
- zgłaszania właściwym organom poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami;
- testowania operacyjnej odporności cyfrowej;
- wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami w tym obszarze;
- środków na rzecz należytego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT;
- wymogów co do umów zawartych między zewnętrznymi dostawcami usług ICT a podmiotami finansowymi;
- zasad wprowadzania nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT świadczącymi usługi na rzecz podmiotów finansowych;
- zasad współpracy między właściwymi organami oraz zasad nadzoru i egzekwowania przepisów przez właściwe organy w odniesieniu do wszystkich kwestii objętych rozporządzeniem.

Wnioski

W obliczu dynamicznego rozwoju technologii cyfrowych i wzrostu liczby zagrożeń cybernetycznych, instytucje finansowe muszą stale doskonalić swoje strategie zarządzania ryzykiem i bezpieczeństwem.

Wprowadzenie regulacji takiej jak DORA jest krokiem w stronę zwiększenia odporności sektora finansowego na cyberzagrożenia.

Jednakże kluczowym elementem skutecznej ochrony pozostaje ścisła współpraca pomiędzy instytucjami finansowymi, regulatorami oraz dostawcami technologii.

Cyberbezpieczeństwo to nie tylko technologia, ale także odpowiednie procedury i świadomość użytkowników oraz pracowników, które razem mogą skutecznie przeciwdziałać zagrożeniom.

Artykuł powstał na podstawie webinarium, które 21 października 2024 r. prowadziła radca prawny Monika Macura, na temat podstawowych zagrożeń, regulacji oraz dobrych praktyk w zakresie cyberbezpieczeństwa dla instytucji finansowych.

Pełne nagranie webinarium „Cyberbezpieczeństwo w rozwiązaniach płatniczych" jest dostępne na kanale youtube kancelarii.

Autor: Monika Macura, radca prawny

Rozporządzenie DORA a małe instytucje płatnicze

Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011, czyli tzw. rozporządzenie DORA (Digital Operational Resilience Act), stanowi kluczowy akt prawny, który regulować będzie zasady operacyjnej odporności cyfrowej i bezpieczeństwa ICT dla całej branży finansowej.

Cele rozporządzenia

Rozporządzenie DORA ma na celu harmonizację przepisów dotyczących operacyjnej odporności cyfrowej i bezpieczeństwa ICT w obszarze usług finansowych. Reguluje w szczególności zasady:

- zarządzania ryzykiem ICT;
- zgłaszania poważnych incydentów związanych z ICT;
- testowania operacyjnej odporności cyfrowej;
- wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami w tym obszarze;
- zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT;
- mające zastosowanie do ustaleń umownych zawartych między zewnętrznymi dostawcami usług ICT a podmiotami finansowymi;
- dotyczące ustanowienia i funkcjonowania ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT świadczącymi usługi na rzecz podmiotów finansowych.

Rozporządzenie DORA obejmie swym zakresem podmioty finansowe, takie jak:

- instytucje kredytowe;
- instytucje płatnicze;
- i dostawców usług w zakresie kryptoaktywów.

Znajdzie zastosowanie do zewnętrznych dostawców usług ICT.

Powstaje jednak pytanie, czy DORA swym zakresem podmiotowym obejmie także i małe instytucje płatnicze?

Zakres przedmiotowy DORA a małe instytucje płatnicze

Zgodnie z artykułem 2 ust. 1 lit b Rozporządzenia DORA, rozporządzenie ma zastosowanie w szczególności do instytucji płatniczych, w tym instytucji płatniczych zwolnionych zgodnie z dyrektywą (UE) 2015/2366. Na podstawie zaś artykułu 3 pkt. 32 rozporządzenia DORA, „instytucja płatnicza zwolniona zgodnie z dyrektywą (UE) 2015/2366" oznacza instytucję płatniczą zwolnioną zgodnie z art. 32 ust. 1 dyrektywy (UE) 2015/2366 (tzw. dyrektywy PSD2).

Małe instytucje płatnicze stanowią właśnie instytucje, których funkcjonowanie oparte jest na zwolnieniu jakie przewiduje dyrektywa PSD2 w art. 32, a które zaimplementowane zostało do porządku prawnego poprzez odpowiednie przepisy działu VI B ustawy o usługach płatniczych.

Oznacza to, że **co do zasady rozporządzenie DORA obejmować będzie również małe instytucje płatnicze.**

Ramy zarządzania ryzykiem związanym z ICT mające zastosowanie do MIP

Rozporządzenie DORA przewiduje jednak w pewnym zakresie odmienne, uproszczone zasady, mające zastosowanie do podmiotów takich jak małe instytucje płatnicze.

W tym celu DORA **ustanawia tzw. uproszczone ramy zarządzania ryzykiem związanym z ICT.** Zgodnie bowiem z art. 16 ust. 1 DORA, ogólne zasady zarządzania ryzykiem ICT nie będą miały zastosowania do małych instytucji płatniczych, jako instytucji zwolnionych zgodnie z dyrektywą 2013/36/UE.

Nie oznacza to jednak, że małe instytucje płatnicze zostaną w pełni zwolnione z obowiązku zarządzania ryzykiem ICT. **W ramach wspominanych uproszonych ram zarządzania ryzykiem związanym z ICT, małe instytucje płatnicze w szczególności:**

- wprowadzają i utrzymują prawidłowe i udokumentowane ramy zarządzania ryzykiem związanym z ICT;
- stale monitorują bezpieczeństwo i funkcjonowanie wszystkich systemów ICT;
- minimalizują wpływ ryzyka związanego z ICT poprzez stosowanie prawidłowych, odpornych i zaktualizowanych systemów, protokołów i narzędzi ICT;
- umożliwiają szybką identyfikację i wykrywanie źródeł ryzyka związanego z ICT i nieprawidłowości w sieci i systemach informatycznych oraz szybkie reagowanie na incydenty związane z ICT;
- określają najważniejsze zależności od zewnętrznych dostawców usług ICT;
- zapewniają ciągłość krytycznych lub istotnych funkcji poprzez plany ciągłości działania oraz środki reagowania i przywracania sprawności;
- regularnie testują ciągłości działania oraz środki reagowania i przywracania sprawności, a także skuteczność działań wdrożonych zgodnie z pkt 1 i 3 powyżej;
- wdrażają, stosownie do przypadku, odpowiednie wnioski operacyjne wynikające z powyższych testów oraz wnioski z analiz przeprowadzonych po wystąpieniu incydentu do procesu oceny ryzyka związanego z ICT;
- opracowują, stosownie do potrzeb i profilu ryzyka związanego z ICT, programy zwiększania świadomości w zakresie bezpieczeństwa ICT oraz szkoleń w zakresie operacyjnej odporności cyfrowej dla pracowników i kadry zarządzającej.

Co istotne EUN (EBA, EIOPA oraz ESMA) zobowiązane zostały do wspólnego opracowania w tym zakresie projektu regulacyjnych standardów technicznych, mających na celu doprecyzowanie wymogów, jakie obowiązywać będą w ramach wspomnianych uroszczonych ram zarządzania ryzykiem związanym z ICT. Finalne projekty powyższych standardów zostały już opracowane w ramach tzw. **pierwszego pakietu aktów wykonawczych do Rozporządzenia DORA** (RTS on ICT risk management framework and on simplified ICT risk management framework).

Pozostałe wymogi DORA mające zastosowanie do MIP

Należy również pamiętać, że poza zasadami zarządzania ryzykiem ICT, rozporządzenie DORA ustanawia szereg dodatkowych zasad i wymogów, w szczególności w zakresie zarządzania incydentami związanymi z ICT (w tym ich klasyfikacją i zgłaszaniem), testowania operacyjnej odporności cyfrowej, jak i zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT.

W tym zakresie Rozporządzenie DORA także przewiduje pewne uproszczenia mające zastosowanie w małych instytucjach płatniczych zwolnionych zgodnie z dyrektywą 2013/36/UE. Powyższe uproszczenia obejmują pewne aspekty testowania narzędzi, systemów i procesów ICT z wykorzystaniem TLPT oraz wymogi co do ustanawiania strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT.

Do małych instytucji płatniczych, potencjalnie zastosowanie mogą znaleźć także pewne wyłączenia i uproszczone zasady przewidziane w przypadku niektórych wymogów i obowiązków dla mikroprzedsiębiorców (mikroprzedsiębiorcą będzie MIP, która to zatrudnia mniej niż 10 osób i której roczny obrót lub bilans roczny nie przekracza 2 mln EUR).

W pozostałym, przeważającym zakresie, wspomniane zasady i wymogi w zakresie zarządzania incydentami związanymi z ICT (w tym ich klasyfikacją i zgłaszaniem), testowania operacyjnej odporności cyfrowej, jak i zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT, znajdują pełne zastosowanie w stosunku do małych instytucji płatniczych.

Podsumowanie

Mimo że dla małych instytucji płatniczych, rozporządzenie DORA przewiduje **pewne wyłączenia i uproszczone ramy** zarządzania ryzykiem związanym z ICT, **wciąż na instytucje te nałożony został szeroki zakres dodatkowych obowiązków i wymogów.**

W szczególności małe instytucje będą musiały:

- wdrożyć co najmniej uproszczone ramy zarządzania ryzykiem związanym z ICT;
- wdrożyć nowe zasady zarządzania incydentami związanymi z ICT, ich klasyfikację i zgłaszanie;
- wdrożyć testowanie operacyjnej odporności cyfrowej;
- zarządzać ryzykiem ze strony zewnętrznych dostawców usług ICT, w tym zapewnić zgodność umów zawartych z dostawcami usług ICT z rozporządzeniem.

Nie ulega zatem wątpliwości, że **każda mała instytucja płatnicza do dnia 17 stycznia 2025 r. musi dostosować się do rozporządzenia DORA i zapewnić zgodność prowadzonej działalności z powyższym rozporządzeniem.**

Już teraz małe instytucje płatnicze powinny zatem rozpocząć proces wdrożenia rozporządzenia DORA, który wymagać będzie aktualizacji dokumentacji wewnętrznej, wdrożenia odpowiednich rozwiązań z zakresu bezpieczeństwa ICT i zarządzania ryzykiem ICT, jak również dostosowaniem relacji umownych łączących MIP z zewnętrznymi dostawcami usług ICT (co w praktyce oznaczać będzie konieczność renegocjowania wielu umów).

Autor: Michał Barwicki, radca prawny

DORA – zarządzanie ryzykiem i incydentami ICT

Kontynuując omówienie zagadnień dotyczących cyberbezpieczeństwa, tym razem omawiamy kwestie związane z zarządzaniem ryzykami w obszarze ICT. Artykuł powstał na podstawie webinarium „Cyberbezpieczeństwo w rozwiązaniach płatniczych", które 21 października 2024 r. prowadziła radca prawny Monika Macura, na temat podstawowych zagrożeń, regulacji oraz dobrych praktyk w zakresie cyberbezpieczeństwa dla instytucji finansowych.

Zarządzanie ryzykiem ICT

Zarządzanie ryzykiem związanym z technologiami informacyjnymi (ICT) jest podstawowym wymogiem wobec instytucji finansowych, korzystających z systemów płatniczych, co obejmuje obowiązki:

- wprowadzenia spójnej organizacji i ram zarządzania ryzykiem ICT;
- zapewnienia, że organ zarządzający podmiotu finansowego określa, zatwierdza i nadzoruje wdrażanie wszystkich ustaleń dotyczących ram zarządzania ryzykiem związanym z ICT;
- stosowania i utrzymywania zaktualizowanych systemów, protokołów i narzędzi ICT;
- identyfikacji, klasyfikacji i dokumentowania funkcji biznesowych opartych na ICT;
- monitorowania i kontroli bezpieczeństwa systemów, protokołów i narzędzi ICT;
- wykrywania, reagowania na incydenty i przywracania sprawności;

- wdrożenia kompleksowej polityki ciągłości działania ICT;
- opracowania i dokumentowania zasad tworzenia kopii zapasowych;
- związane z okresowymi przeglądami raportowaniem i doskonaleniem.

Zarządzanie incydentami ICT

Obejmuje przede wszystkim obowiązek ustanowienia środków w celu wykrywania, zarządzania, rejestrowania i powiadamiania o incydentach związanych z ICT oraz właściwej klasyfikacji incydentów pod kątem ustalonych kryteriów, a także zgłaszanie poważnych incydentów związanych z ICT wyznaczonemu właściwemu organowi i ujednolicenie raportowania incydentów związanych z usługami płatniczymi (PSD2).

Testowanie odporności cyfrowej

Dotyczy obowiązków w zakresie:
- ustanowienia, utrzymywania i weryfikacji solidnych i kompleksowych programów testowania operacyjnej odporności;
- testowania narzędzi i systemów ICT;
- przeprowadzania okresowych testów penetracyjnych;

a także zaawansowanego testowania narzędzi, systemów i procesów ICT z wykorzystaniem TLPT (testy penetracyjne pod kątem wyszukiwania zagrożeń).

Ramy dokumentacji prawnej w zarządzaniu ryzykiem ICT obejmują:
- politykę zarządzania ryzykiem;
- strategię operacyjnej odporności cyfrowej;
- politykę bezpieczeństwa;
- politykę ciągłości działania / plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej (tzw. disaster recovery);
- proces zarządzania incydentami, w tym procedury reagowania na incydenty;
- procedurę testowania operacyjnej odporności cyfrowej;
- strategię dotycząca ryzyka związanego z usługami ICT, w tym ryzyk ze strony zewnętrznych dostawców usług ICT;
- procedury tworzenia kopii zapasowych, a także procedury i metody przywracania i odzyskiwania danych;
- inne wymagane dokumenty opisujące system zarządzania bezpieczeństwem informacji.

Zarządzanie ryzykiem ze strony zewnętrznych dostawców ICT

Obowiązek zarządzania ryzykiem stron trzecich jest integralnym elementem ogólnego ryzyka ICT i obejmuje:

- obowiązek zapewnienia zgodności zawartych umów dotyczących usług ICT z ustanowionymi wymogami;
- obowiązek prowadzenia rejestru umów.

Outsourcing usług płatniczych

Powierzenie wykonywania określonych czynności operacyjnych związanych ze świadczeniem usług płatniczych lub z działalnością w zakresie wydawania pieniądza elektronicznego (w tym czynności istotnych) określone jest w **art. 86 Ustawy o usługach płatniczych**.
Warto zwrócić uwagę na **warunki powierzenia usług płatniczych insoucerowi**, zgodnie z którymi:

- powierzenie nie wpłynie niekorzystnie na prowadzenie przez spółkę działalności zgodnie z przepisami prawa i wydanym jej zezwoleniem oraz na ostrożne i stabilne zarządzanie spółką;
- insourcer posiada uprawnienia do wykonywania czynności w zakresie przedmiotu umowy;
- insourcer posiada niezbędną wiedzę i doświadczenie oraz zapewnia warunki techniczne i organizacyjne niezbędne do prawidłowego wykonywania umowy outsourcingu, a w szczególności posiada odpowiedni system zarządzania ryzykiem, w standardzie nie niższym niż wymagany od instytucji płatniczej, odpowiednią infrastrukturę techniczną i technologiczną, zdolność raportowania obejmującą informacje na temat procesu świadczenia usług zgodnie z wymogami spółki;
- sytuacja finansowa insourcera pozwala na prawidłowe wykonywanie umowy;
- insourcer umożliwi skuteczne nadzorowanie przez spółkę wykonywania powierzonych mu czynności oraz zarządzanie ryzykiem związanym z powierzeniem czynności;
- spółka będzie posiadać dostęp do informacji i dokumentów związanych z wykonywaniem czynności powierzonych insourcerowi;
- spółka posiada plan działania zapewniające ciągłe, bezpieczne i niezakłócone prowadzenie działalności w zakresie objętym umową, również w przypadku rozwiązania umowy.

Reżim outsourcingu uzupełniają akty prawa miękkiego – tzw. soft law, w tym:

- Rekomendacja D KNF dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach;
- Rekomendacja M KNF dotycząca zarządzania ryzykiem operacyjnym w bankach;
- Wytyczne EBA ws. outsourcingu z 25.02.2019 r.;
- Wytyczne EBA ws. ICT i zarządzania ryzykiem bezpieczeństwa z 28.11.2019 r.;
- Stanowisko UKNF ws. outsourcingu;
- Komunikat UKNF ws. chmury obliczeniowej oraz moduł Q&A w zakresie stosowania Komunikatu UKNF ws. chmury obliczeniowej.

W związku z wejściem **w życie Rozporządzenia DORA**, **KNF wyraził zamiar uchylenia w przyszłości część aktów prawa miękkiego** dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego **m.in. Rekomendacji D czy też Komunikatu Chmurowego KNF**.

Polityka w zakresie korzystania z usług dostawców ICT powinna określać:

- środki i kluczowe wskaźniki służące bieżącemu monitorowaniu wyników zewnętrznych dostawców usług ICT;
- zasady przekazywania sprawozdań działań i usług;
- zasady oceny wyników dostawców ICT za pomocą kluczowych wskaźników efektywności, kluczowych wskaźników kontroli, audytów, samocertyfikacji i niezależnych przeglądów;
- zasady powiadamiania o incydentach;
- środki stosowane przez podmiot finansowy w przypadku stwierdzenia niedociągnięć ze strony dostawcy ICT;
- plan wyjścia z umowy z dostawcą ICT, obejmujący min. nieprzewidziane i trwałe przerwy w świadczeniu usług, świadczenie usług w sposób nieodpowiedni lub brak świadczenia usług, niespodziewane wypowiedzenie ustalenia umownego;
- zasady zawierania umów z dostawcami usług ICT wspierających krytyczne lub kluczowe funkcje i wyznaczenie osoby odpowiedzialnej;
- rodzaj usług ICT, miejsce jej świadczenia, siedzibę dostawcy usługi ICT, wzmiankę o przynależności dostawcy do grupy;

- charakter danych przekazywanych dostawcy ICT;
- zasady korzystania z usług dostawcy ICT, posiadającego zezwolenie na świadczenie usług w innym państwie członkowskim;
- ryzyko uzależnienia od zewnętrznych dostawców ICT;
- zasady migracji usług ICT do innego dostawcy;
- wpływ zakłóceń w świadczeniu usług ICT na ciągłość działania podmiotu finansowego;
- zasady audytu i zewnętrznego przeglądu dostawców usług ICT;
- zasady oceny ryzyka dostawcy ICT;
- zapisy umowne – wzorcowe klauzule.

Jakie mogą być funkcje usługi ICT?

Przede wszystkim, **ICT development**, czyli świadczenie usług związanych z analizą biznesową i projektowaniem. **ICT helpdesk** zajmuje się tworzeniem i testowaniem oprogramowania. **ICT security management services** obejmuje świadczenie usług związanych ze wsparciem helpdesku i wsparciem w zakresie incydentów ICT. ICT security management services obejmuje bezpieczeństwo ICT, czyli ochronę, wykrywanie, reagowanie, odzyskiwanie i obsługę incydentów bezpieczeństwa.

Wśród innych funkcji warto wymienić:

- **Provision of data** – usługa dostawców danych;
- **Data analisys** – usługi wsparcia analizy danych;
- **ICT facilities and hosting** – zapewnienie infrastruktury ICT, obiektów i usług hostingowych;
- **Computation** – zapewnienie możliwości przetwarzania cyfrowego;
- **Non-Cloud Data storage** – zapewnienie platformy przechowywania danych (z wykluczeniem usług w chmurze);
- **Telecom carrier** – operacje dla systemów telekomunikacyjnych i zarządzanie przepływem;
- **Network infrastructure** – zapewnienie infrastruktury sieciowej;
- **Hardware and physical devices** – dostarczanie stacji roboczych, telefonów, serwerów, urządzeń do przechowywania danych;
- **Software licensing** – dostarczanie oprogramowania działającego lokalnie;
- **ICT operation management** – świadczenie usług związanych z konfiguracją infrastruktury, konserwacją, instalacją, zarządzaniem pojemnością;

- **ICT Consulting** – świadczenie usług w zakresie wiedzy ICT;
- **ICT risk management** – weryfikacja zgodności z wymogami zarządzania ryzykiem;
- **ICT project management** - świadczenie usług związanych z funkcją kierownika projektu;
- **Usługi Infrastructure-as-a-Service / Usługi Platform-as-a-Service / Usługi Software-as-a-Service.**

Wzorcowe klauzule umowne – wytyczne ZBP

Wzorcowe klauzule, dotyczące współpracy w zakresie dostawców wspierających usługi krytyczne lub istotne obejmują zasady i postanowienia dotyczące:

- wypowiadania umowy;
- określenia miejsca świadczenia usług;
- bezpieczeństwa danych i zasady informowania o incydentach związanych z bezpieczeństwem danych;
- dostarczania raportów z obszaru bezpieczeństwa teleinformatycznego oraz środków i testów ciągłości działania;
- zwrotu, usunięcia i dostępu do danych;
- współpracy dostawcy z podmiotem finansowym;
- przeprowadzania testów penetracyjnych;
- przeprowadzania audytu (w tym audytów środków kontroli wewnętrznej i audytów finansowych;

a także alternatywne poziomy zabezpieczeń, obowiązki dostawcy w kontekście umowy z podwykonawcami, plany reagowania na incydenty i plany ciągłości działania, strategie wyjścia oraz gwarantowany poziom jakości usług (SLA).

Autor: Monika Macura, radca prawny

Wdrożenie DORA – wnioski praktyczne

W cyklu poświęconym omówieniu zagadnień dotyczących cyberbezpieczeństwa tym razem dzielimy się praktycznymi wnioskami na temat wdrożenia DORA. Zachęcamy też do obejrzenia webinarium „Cyberbezpieczeństwo w rozwiązaniach płatniczych", które 21 października 2024 r. prowadziła radca prawny Monika Macura, na temat podstawowych zagrożeń, regulacji oraz dobrych praktyk w zakresie cyberbezpieczeństwa dla instytucji finansowych.

Audyt spełnienia wymagań Rozporządzenia DORA

Pierwszy krok to weryfikacja systemu zarządzania ryzykiem pod kątem uwzględnienia kwestii ICT jako części ryzyka operacyjnego.

Kolejny etap powinien objąć ocenę zgodności planu ciągłości działania z wymogami DORA, zwłaszcza weryfikację, na ile uwzględnia on zakres wymagany przez DORA.

W dalszym etapie oceniamy pod względem zgodności z DORA:

- zarządzanie incydentami związanymi z ICT;
- program testowania operacyjnej odporności cyfrowej;
- wewnętrzne polityki i regulacje.

Z doświadczenia – zmiany lub opracowanie obejmą następujące dokumenty:

- strategię odporności cyfrowej;
- politykę bezpieczeństwa informacji;
- politykę ciągłości działania;
- proces zarządzania incydentami, w tym procedurę reagowania na incydenty;
- program testowania operacyjnej odporności cyfrowej;
- strategię dotyczącą ryzyka związanego z usługami ICT, w tym ryzyk ze strony zewnętrznych dostawców usług ICT;
- procedurę tworzenia kopii zapasowych, a także procedury i metody przywracania i odzyskiwania danych.

Określenie wymogów technicznych w zakresie odporności cyfrowej – szkolenia pracowników i osób zarządzających

DORA wymaga od instytucji finansowych regularnego testowania swoich systemów ICT w celu oceny ich odporności na cyberzagrożenia, co obejmuje:

- **regularne testy penetracyjne** oraz bardziej zaawansowane testy, które mają na celu identyfikację słabych punktów w systemach oraz procedurach bezpieczeństwa;
- **testowanie narzędzi i systemów ICT** oraz ich funkcji krytycznych, aby upewnić się, że organizacja jest w stanie szybko przywrócić usługi po ewentualnym incydencie.

Programy testowania operacyjnej odporności pozwalają na ocenę skuteczności środków ochrony oraz doskonalenie strategii przeciwdziałania zagrożeniom.

Współpraca z zewnętrznymi dostawcami usług ICT

Jak omawialiśmy w poprzednim artykule, instytucje finansowe często korzystają z usług zewnętrznych dostawców ICT, co wiąże się z koniecznością zarządzania ryzykiem związanym z outsourcingiem.

Kluczowe wyzwania obejmują:

- ocenę zgodności umów zawartych z dostawcami usług ICT z wymogami prawnymi oraz polityką bezpieczeństwa instytucji finansowej;
- zarządzanie ryzykiem koncentracji ICT, czyli uzależnieniem od jednego lub kilku dostawców, co może wpłynąć na dostępność usług w przypadku ich problemów operacyjnych;
- wprowadzenie klauzul umownych dotyczących bezpieczeństwa, procedur raportowania oraz reagowania na incydenty, co jest szczególnie ważne w kontekście świadczenia usług krytycznych dla funkcjonowania instytucji.

Regulacje takie jak DORA nakładają na instytucje finansowe obowiązek monitorowania i oceny ryzyka związanych z dostawcami ICT oraz wdrażania środków zaradczych w przypadku stwierdzenia niedociągnięć.

Outsourcing usług płatniczych i soft law

W kontekście outsourcingu usług płatniczych należy uwzględnić przepisy prawa, jak i akty prawa miękkiego, które regulują zarządzanie ryzykiem:

- **art. 86 Ustawy o usługach płatniczych** określa warunki, jakie muszą spełniać instytucje powierzające swoje czynności operacyjne podmiotom trzecim;
- **rekomendacje i wytyczne**, takie jak Rekomendacja D KNF dotycząca bezpieczeństwa ICT w bankach czy Wytyczne EBA w zakresie outsourcingu, wskazują na najlepsze praktyki w zakresie zarządzania ryzykiem.

Wytyczne te obejmują nie tylko kwestie techniczne, ale również prawne i operacyjne, które mają na celu minimalizowanie ryzyka związanego z wykorzystaniem usług zewnętrznych dostawców.

Polityka korzystania z usług dostawców ICT

Współpraca z dostawcami usług ICT wymaga szczególnej uwagi w zakresie zarządzania ryzykiem. Polityka dotycząca korzystania z usług tych dostawców powinna uwzględniać:

- kluczowe wskaźniki efektywności i kontroli służące do monitorowania jakości świadczonych usług;
- zasady przekazywania raportów oraz powiadamiania o incydentach związanych z bezpieczeństwem danych;
- plany wyjścia z umowy, które określają procedury działania w przypadku zakończenia współpracy z dostawcą ICT, aby uniknąć zakłóceń w świadczeniu usług.

Dokumentacja dotycząca polityki bezpieczeństwa i zarządzania ryzykiem musi być na bieżąco aktualizowana i zgodna z obowiązującymi przepisami.

Podsumowanie

Cyberbezpieczeństwo w rozwiązaniach płatniczych wymaga zintegrowanego podejścia obejmującego zarówno regulacje prawne, zarządzanie ryzykiem, jak i najlepsze praktyki operacyjne.

Nowe regulacje, takie jak DORA, podnoszą standardy bezpieczeństwa w sektorze finansowym, jednak ich skuteczność zależy od wdrożenia odpowiednich procedur oraz współpracy między instytucjami a dostawcami technologii.

W obliczu dynamicznego rozwoju zagrożeń cybernetycznych, niezbędne jest również podnoszenie świadomości pracowników oraz ciągłe doskonalenie strategii ochrony przed atakami.

Autor: Monika Macura, radca prawny

Stanowisko UKNF w sprawie DORA

31 grudnia 2024 r. opublikowane zostało Stanowisko Urzędu Komisji Nadzoru Finansowego (UKNF), dotyczące stosowania przez podmioty finansowe Rozporządzenia DORA. Mimo braku przepisów zapewniających stosowanie Rozporządzenia DORA, nie należy przyjmować, że następuje wstrzymanie obowiązku przestrzegania przez podmioty finansowe wymogów, wynikających z wyżej wspomnianego rozporządzenia, które zacznie obowiązywać już od 17 stycznia 2025 r.

Rozporządzenie DORA weszło w życie 16 stycznia 2023 r., dając podmiotom finansowym 2 lata na dostosowanie się do jego wymogów. Okres ten zakończy się 16 stycznia 2025 r.

Jak zostało wskazane we wspomnianym stanowisku „UKNF oczekuje, że począwszy od dnia rozpoczęcia stosowania Rozporządzenia DORA podmioty finansowe będą stosowały się do sposobu i trybu wykonywania określonych obowiązków informacyjnych i sprawozdawczych zgodnie z niniejszym stanowiskiem".

W niniejszym artykule omawiamy nowe obowiązki dla podmiotów finansowych.

Obowiązek posiadania identyfikatora LEI jako niezbędnego elementu sprawozdawczości

Zgodnie z obowiązkami, wynikającymi z Rozporządzenia DORA, podmioty finansowe są zobowiązane do posiadania tzw. identyfikatora LEI od 17 stycznia 2025 r.

Podmioty finansowe, które jeszcze go nie posiadają, powinny wystąpić o jego uzyskanie i uzyskać go przed dniem 17 stycznia 2025 r., czyli przed datą rozpoczęcia stosowania Rozporządzenia DORA.

Brak posiadania identyfikatora LEI uniemożliwi przekazanie formularzy sprawozdawczych do KNF jako właściwego organu, a następnie do przekazania części z nich przez KNF do Europejskich Urzędów Nadzoru.

Brak identyfikatora LEI należy traktować jako niedopełnienie obowiązku w zakresie sprawozdawczości, co oznacza niedostosowanie się do Rozporządzenia DORA. **W konsekwencji na podmiot finansowy mogą zostać nałożone sankcje**, poczynając od najmniej dotkliwych w formie publicznej nagany, po karę grzywny oraz w skrajnych przypadkach wycofanie licencji na działalność nadzorowaną.

W Polsce **kod LEI** można uzyskać za pośrednictwem **Krajowego Depozytu Papierów Wartościowych S.A.** (KDPW).

Obowiązki sprawozdawcze od 17 stycznia 2025 r.

W pierwszej kolejności podmioty finansowe powinny być przygotowane do realizowania określonych obowiązków sprawozdawczych w zakresie obejmującym min.: wstępne powiadomienie i sprawozdania dotyczące poważnych incydentów ICT (SPR-PF-07), powiadomienie o znaczącym cyberzagrożeniu (SPR-PF-10) czy w zakresie pełnego rejestru informacji lub innego zakresu informacji zgodnie z żądaniem (SPR-PF-18).

Więcej na ten temat w samym Stanowisku UKNF dotyczącym stosowania przez podmioty finansowe Rozporządzenia DORA.

Ponadto, jak wskazuje UKNF, obowiązki sprawozdawcze powinny być realizowane w postaci elektronicznej, z wykorzystaniem kanałów komunikacji, w tym systemów teleinformatycznych i narzędzi teleinformatycznych udostępnionych przez UKNF, takich jak:

- System Sprawozdawczości DORA;
- System do zgłaszania poważnych incydentów związanych z ICT;
- kanał do komunikacji i wymiany informacji w zakresie testów TLPT, uzgodniony z podmiotem finansowym realizującym test.

Wyraźnie widać rosnącą tendencję do stosowania odpowiednich systemów i automatyzacji procesów sprawozdawczych.

Zgłaszanie poważnych incydentów związanych z ICT oraz znaczących cyberzagrożeń

Zgodnie z Rozporządzeniem DORA *„**incydent związany z ICT**”* został zdefiniowany jako: *„(...) pojedyncze zdarzenie lub seria powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy”*.

Jako definicję *„**poważnego incydentu związanego z ICT**”* należy wskazać *„incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego”*. Ponadto, zgodnie z Rozporządzeniem DORA, UKNF w sprawozdaniu zaznacza szereg kryteriów w zakresie klasyfikacji poważnych incydentów związanych z ICT, w tym m.in.:

- liczbę lub znaczenie klientów lub kontrahentów finansowych oraz (w stosownych przypadkach) kwotę lub liczbę transakcji, których dotyczy incydent związany z ICT, oraz to czy taki incydent spowodował skutki reputacyjne;
- czas trwania incydentu związanego z ICT, w tym przerwę w świadczeniu usług;
- zasięg geograficzny incydentu związanego z ICT, w szczególności, jeżeli dotyczy on więcej niż dwóch państw członkowskich.

Więcej na ten temat w treści Stanowiska UKNF dotyczącego stosowania przez podmioty finansowe Rozporządzenia DORA.

Klasyfikacja incydentów związanych z ICT, w tym ocena wystąpienia poważnego incydentu, powinna opierać się na definicji „poważnego incydentu związanego z ICT" oraz na kryteriach klasyfikacji i progach istotności określonych w regulacyjnych standardach technicznych. Wynika to z konieczności zapewnienia maksymalnej efektywności przepisów prawa unijnego.

Rozporządzenie DORA przewiduje wyłączenie obowiązku zgłaszania incydentów zgodnie z dyrektywą PSD2 w stosunku do dostawców usług płatniczych, objętych zakresem stosowania Rozporządzenia DORA.

Podmioty nadzorowane, wymogiem raportowania incydentów na podstawie dyrektywy PSD2, będą zobowiązane do zgłaszania poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami zgodnie z Rozporządzeniem DORA.

Ponadto, operatorzy usług kluczowych, do czasu uchwalenia przepisów implementujących dyrektywę NIS2, powinni równolegle, (niezależnie od zgłaszania poważnych incydentów związanych z ICT), przekazywać zgłoszenia incydentów poważnych w sposób przewidziany w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Prowadzenie i przekazanie rejestru informacji dotyczącego umów z zewnętrznymi dostawcami usług ICT

Zgodnie ze sprawozdaniem UKNF – właściwe organy będą zobowiązane pozyskać od podmiotów finansowych rejestry informacji w terminie umożliwiającym przekazanie zebranych danych do Europejskiego Urzędu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych oraz Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EUN) **przed 30 kwietnia 2025 r.**

W związku z powyższym KNF planuje zwrócić się **na początku kwietnia 2025 r.**, do podmiotów finansowych z żądaniem przekazania rejestrów informacji do KNF, tak aby KNF mogła terminowo zrealizować obowiązek przekazania zebranych rejestrów informacji do EUN.

Podkreślono, że przekazywane w 2025 r. do właściwych organów rejestry informacji **powinny zawierać dane aktualne na 31 marca 2025 r.**

Kluczowe znaczenie ma również rozporządzenie wykonawcze Komisji (UE) 2024/2956 z dnia 29 listopada 2024 r., ustanawiające wykonawcze standardy techniczne do celów stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do standardowych wzorów na potrzeby rejestru informacji z uwagi na doprecyzowanie, jakie dane powinny się w nim znaleźć, a w konsekwencji, jakie informacje będą przekazywane do właściwego organu.

Prowadzenie i przekazanie rejestru informacji dotyczącego umów z zewnętrznymi dostawcami usług ICT

Zgodnie ze stanowiskiem planowane jest również uchylenie:

- Rekomendacji D, dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach;
- Rekomendacji D-SKOK, dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych;

oraz wytycznych dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w:

- zakładach ubezpieczeń i zakładach reasekuracji;
- towarzystwach funduszy inwestycyjnych;
- firmach inwestycyjnych;
- podmiotach infrastruktury rynku kapitałowego.

Ponadto, planowane jest również odwołanie komunikatu UKNF dotyczącego przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej – tzw. Komunikat chmurowy.

Autor: Oliwia Pawłowska, asystent prawny

MACURA.

O kancelarii

Jesteśmy wyspecjalizowaną kancelarią prawną. Od 2012 r. skutecznie **doradzamy podmiotom z sektora FinTech, LendTech, e-commerce oraz nowych technologii.** Inspirujemy i wspieramy klientów we wprowadzaniu innowacyjnych rozwiązań.

Rozumiemy nie tylko prawne ale także technologiczne i finansowe aspekty działalności naszych klientów, więc stanowimy doskonały wybór dla firm poszukujących wyspecjalizowanej wiedzy i partnerstwa.

Ekspercką wiedzę i innowacyjne podeście potwierdzają **rekomendacje dla kancelarii i jej ekspertów w prestiżowych rankingach – międzynarodowym rankingu Chambers FinTech Legal 2025** oraz ogólnopolskim **Rankingu Rekomendacji Kancelarii Prawniczych Rzeczpospolitej** 2023 w dziedzinach TMT, prawo bankowe i finansowe oraz ochrona prywatności i danych osobowych.

Doradzamy, chronimy i inspirujemy innowacje finansowe

MACURA.

Chambers RANKED IN FinTech 2025 Kancelaria Macura

POROZMAWIAJMY.

Monika Macura
T: (+48) 696-011-713
M: monika.macura@kancelariamacura.pl

MONIKA MACURA
KANCELARIA RADCY PRAWNEGO
ul. Odyńca 7/13, 02-606 Warszawa
www.kancelariamacura.pl

#cyberbezpieczeństwo
#NoweTechnologie